System-Level Controls for the Internal Revenue Service's Mainframe Computers Are Generally Adequate; However, Additional Actions Are Needed

September 2002

Reference Number: 2002-20-168

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 4, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION & CHIEF INFORMATION OFFICER

FROM: Pamela J. Gardiner
Acting Inspector General

SUBJECT: Final Audit Report - System-Level Controls for the Internal Revenue Service's Mainframe Computers Are Generally Adequate; However, Additional Actions Are Needed (Audit # 200220003)

This report presents the results of our review of the system-level controls over the Internal Revenue Service's (IRS) mainframe computers. The overall objective of this review was to determine whether issues presented in previous Treasury Inspector General for Tax Administration (TIGTA) audit reports, when viewed as a whole, indicate the need for broader management actions across all mainframe computer environments.

In summary, we found that the system-level controls over the IRS' mainframe computers were generally adequate. Specifically, our audits determined that the IRS either had in place adequate system-level controls for its mainframe computers or was taking steps to improve them. In particular, we determined that controls over user access to these mainframe computers were generally adequate. In addition, we determined that most of the sensitive programs and data residing on the IRS' mainframe computers were also adequately protected.

While specific weaknesses and areas of improvement in system-level controls were identified for individual mainframe computers, these issues do not constitute an overall weakness in the system-level control environment for the IRS' mainframe computers. However, a common cause for many of these issues is the lack of current and/or complete access control standards for the IRS' mainframe computers, some of which have not been updated for over 5 years. By not timely updating access standards for its mainframe computers, the IRS does not meet General Accounting Office requirements that Federal agencies are to maintain and periodically update documentation of their internal control structure. Access standards need to be periodically updated in order to reflect changes to a computer's configuration or an organization's business processes.

Without current standards, the IRS risks continuing to grant system users higher levels of access to its mainframe computers than they need to do their jobs. In addition, the lack of current standards could complicate disaster recovery efforts. Without current standards, which ensure that mainframe computers are administered consistently, time may be needed to gain an understanding of an individual computer's unique security configuration in order to adequately secure a recovered mainframe. Given that the IRS' mainframe computers are vital to accomplishing its mission, these systems need to be secured as quickly as possible.

Despite the importance of access standards to the security of the IRS' mainframe computers, the IRS has not made the update of these standards a priority. The IRS has often delayed planned corrective actions to update these standards in response to prior TIGTA reports. In addition, the progress of revising these standards is not tracked or monitored by Modernization, Information Technology, and Security (MITS) Services executive management.

Our audits of the operating system software configuration on several of the IRS' mainframe computers found the controls to also be generally adequate. However, two common weaknesses were identified with key system libraries containing computer programs, which could have adversely affected the security and integrity of the computers.

At the time of our audits, the IRS did not use a system-software monitoring tool, such as the one the TIGTA used during these audits. Such a monitoring tool would greatly increase the IRS' ability to maintain adequate system software control, through the automation of routine analysis and monitoring of the key system software. This would enable systems programming and security personnel to more efficiently identify system software issues and focus their efforts on resolving those issues, therefore providing additional time to devote to other priorities.

To further improve the system-level controls over the IRS' mainframe computers, we recommend that the Deputy Commissioner for Modernization & Chief Information Officer ensure that the progress in timely developing and maintaining mainframe computer access control standards is overseen and tracked by MITS Services management. In addition, we recommend that the Chief, Information Technology Services evaluate the use of automated tools to more effectively monitor and maintain the operating system software on the IRS' mainframe computers and establish operating procedures for using such tools to periodically monitor mainframe operating system software.

Management's Response: IRS management agreed with the recommendations presented in this report. Corrective actions will be taken to identify necessary updates to mainframe access controls standards on a quarterly basis and oversee the development of mainframe access control matrices as well as their compliance with standard access control principles. Office of Security Services management will monitor these actions on a quarterly basis. In addition, the IRS will evaluate the use of automated tools to more effectively monitor and maintain the operating system software on the IRS' mainframe computers. The IRS will also establish operating procedures for

using automated tools to periodically monitor mainframe operating system software. Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

System-Level Controls for the Internal Revenue Service's Mainframe Computers Are Generally Adequate; However, Additional Actions Are Needed

Background

The Internal Revenue Service (IRS) relies on a complex environment of computer systems to accomplish its mission. The foundation of this environment is the IRS' mainframe computers, which are based on one of three distinct mainframe operating systems: IBM's operating system 390 (OS/390), IBM's transaction processing facility (TPF), and Unisys' operating system 2200 (OS2200).

The IRS' mainframe computers provide a variety of services for the agency. In particular, these computers:

- Process the nation's tax returns, of which there were approximately 130 million individual income tax returns and 7.6 million business income tax returns processed in Fiscal Year (FY) 2001.
- Support the IRS' customer service efforts by providing taxpayer account information to designated IRS employees.
- Host IRS financial and administrative systems.

This report summarizes our overall assessment of the system-level controls over the IRS' mainframe computers. These controls include access to mainframe computer resources and the configuration of operating system software. Information contained in this report is based on eight Treasury Inspector General for Tax Administration (TIGTA) reports issued since FY 1999 on the adequacy of the system-level controls over the IRS' mainframe computers. A list of these reports is included in Appendix I. Each of these audits was conducted in accordance with *Government Auditing Standards.* Detailed information on our audit objective, scope, and methodology is also presented in Appendix I. Major contributors to the report are listed in Appendix II.

System-Level Controls for the Internal Revenue Service's Mainframe Computers Are Generally Adequate

Overall, the system-level controls over the IRS' mainframe computers are generally adequate. While specific weaknesses and areas of improvement in system-level controls were identified for individual computers, these issues do not constitute an overall weakness in the system-level control environment for these computers. The IRS agreed to take action to correct the issues we reported. In some instances, IRS security personnel took immediate

action to correct identified weaknesses.

Specifically, our audits determined that the IRS either had in place adequate system-level controls for its mainframe computers or was taking steps to improve them. In particular, we determined that controls over user access to these mainframe computers were generally adequate. In addition, we determined that most of the sensitive programs and data residing on the IRS' mainframe computers were also adequately protected. For the three types of mainframe computers used by the IRS, we also identified the following:

- OS/390-based computers: The operating system software configurations of these computers were adequately controlled, which provides reasonable assurance that access controls for these computers will not be circumvented and compromise their integrity.
- TPF-based computers: The IRS is improving the security of these computers by increasing password complexity, developing reports to monitor user activity, and automatically preventing user access for those who do not use the systems after a specified period of time.
- OS2200-based computers: In general, access to sensitive taxpayer data files was adequately protected and user access to these files was reported to management.

Documented Access Control Standards for Mainframe Computers Are Not Timely Updated

Our audits of the access controls over the IRS' mainframe computers identified several weaknesses and areas for improvement for specific computers. These issues included the need to increase the complexity of user passwords; limit unnecessary access to powerful system commands, programs, or data files; and improve the reporting of user mainframe activity to management. These weaknesses provide the opportunity for inadvertent or intentional user actions that could result in unauthorized access to sensitive information or modification of operating system files that could halt computer operations.

Our audits determined that many of these weaknesses could have been prevented with current and/or complete access

control standards for the IRS' mainframe computers. However, the IRS has only completed the update of one of these standards. The IRS organizes its access control standards by mainframe operating system. These standards include access control matrices, which specify the types of access users should be granted, and law enforcement manuals, which specify security requirements for a system. IRS security personnel use these access control standards to administer security on the IRS' mainframe computers.

The Office of Management and Budget (OMB) Circular A-123, "Management Accountability and Control," requires that Federal agencies and individual Federal managers must take systematic and proactive measures to ensure that Federal programs and operations are adequately controlled. The General Accounting Office's (GAO) *Standards for Internal Control in the Federal Government,* and the accompanying *Internal Control Management and Evaluation Tool*, provides that an agency's internal control structure be documented and that such documentation be properly managed, maintained, and periodically updated. These standards also provide that such documentation include the specifics of system and application controls for automated information systems.

The GAO provides additional guidelines for computer system security policies and plans in its *Federal Information System Controls Audit Manual* (FISCAM). Specifically, FISCAM provides that "to be effective, [security] policies and plans should be maintained to reflect current conditions. They should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in agency mission or the types and configuration of computer resources in use. Revisions to the plan should be reviewed, approved, and communicated to all employees. Outdated policies and plans not only reflect a lack of top management concern, but also may not address current risks and, therefore, may be ineffective."

The IRS has not complied with OMB and GAO requirements to maintain and periodically update the internal control structure of its mainframe computers, as documented in access control standards. In some cases, as

the following chart illustrates, the IRS has not updated these standards for over 5 years:

Status of Access Standards for the IRS' Mainframe Computers

Standards	Date of Last Update	Next Issuance Date	Years Between Updates
OS/390 Law Enforcement Manual	February 1998	Completed, January 2002	3 years, 11 months
OS/390 Access Control Matrices	February 1998	May 2003	5 years, 3 months
TPF Access Control Standards	July 1994	July 2002[1]	8 years
OS2200 Law Enforcement Manual	March 2001[2]	March 2003	2 years
OS2200 Access Control Matrix	July 1996	December 2003	7 years, 5 months

Sources: The Department of the Treasury's Inventory, Tracking and Closure System, OS/390 Law Enforcement Manual, and TIGTA Final Reports, as listed in Appendix I to this report.

Access standards need to be periodically updated in order to reflect changes to a computer's configuration or an organization's business processes. For example, the following changes to the IRS' mainframe computers were identified that require access standards to be updated:

- Numerous operating system upgrades were applied to mainframe computers using the TPF operating system over the course of several years, which resulted in the addition of 160 system commands that could be assigned to users. These additional commands were not reflected in the access control standards at the time of our review. In addition, new security features were added to the mainframe

[1] IRS management advised us that the completion date for this standard will be delayed.
[2] Development of the OS2200 law enforcement manual began in March 2001 and is due to be completed in January 2003.

computers that were also not reflected in the standards. Revised access standards provide up-to-date information that guide security personnel in how to properly secure the updated computer system, which in this case would include the types of users that should have access to the new commands and how to use the new security features.

- From 1998 to 2000, the IRS consolidated the operations of many of its mainframe computers. This resulted in significant changes to the configuration and security of these systems. The process for updating several of the access standards for these computers as a result of these changes is still ongoing.

While the access controls for the IRS' mainframe computers are complex and require sufficient time to adequately assess and document, timely and current standards are needed to ensure that the computers continue to be adequately secured. In particular, the IRS risks the following without complete and up-to-date access standards:

- Users with excessive levels of access: Without current standards that account for changes to its mainframe computers, the IRS risks granting users higher levels of access to its mainframe computers than necessary to perform their duties. We identified these types of weaknesses to some degree on all of the IRS' mainframe computers and determined that these control weaknesses were primarily a result of outdated or incomplete access standards. Granting users such levels of access risks the unauthorized access or inadvertent deletion of key system or data files.

- Complicating disaster recovery efforts: Timely and updated access control standards are also needed to support the IRS' disaster recovery and business resumption efforts. Access control standards ensure that mainframe computers are administered consistently, which allows computers to be restored more rapidly during a crisis. Without such standardization, time may be needed to gain an

understanding of an individual computer's unique security configurations in order to adequately secure a recovered mainframe. Given that the IRS' mainframe computers are vital to accomplishing its mission, these systems need to be recovered as quickly as possible.

- Loss of experience: IRS security personnel have made a commendable effort in securing the IRS' mainframe computers without current and up-to-date access control standards. However, as security personnel retire or leave the IRS, their expertise and experience in securing the IRS' mainframe computers is lost. Without current standards to guide new security personnel, systems vulnerabilities will likely increase.

The lack of current and up-to-date access standards for the IRS' mainframe computers is a result of the lack of priority given to maintaining these standards by the IRS. Although the TIGTA has recommended updating these standards, the IRS has delayed implementing several of the corrective actions to these recommendations. For example, the IRS agreed in May 2000 to update the OS2200 access matrices by April 2001. However, a task group was not formed until March 2001 to further develop a law enforcement manual for OS2200-based computers. The next month, April 2001, the corrective action for updating the OS2200 access matrices was delayed to April 2003, in order to include them in the new law enforcement manual. Overall, the IRS has delayed 31 of its 85 corrective actions to TIGTA recommendations regarding access controls for the IRS' mainframe computers. For 24 of these corrective actions, the IRS' delays will result in corrective actions being completed over a year after the TIGTA's report was issued. See Appendix IV for additional information regarding the status of the IRS' corrective actions.

In addition, update of these access standards is not included as a priority effort tracked by the IRS, which would help ensure that these standards are timely updated. Modernization, Information Technology, and Security (MITS) Services executive management oversees the

organization's major initiatives, including computer security, through quarterly business process reviews (BPR). The BPR reports track the status of the organization's initiatives, including progression towards meeting key deadlines. While the BPR reports from October 2001 to May 2002 track the status of initiatives to maintain and enhance security policies, the progress of revising access control standards for the IRS' mainframe computers is not specifically included. Given the length of time between revisions of these standards, the progress of updating the access standards should be more closely tracked by MITS Services management.

Recommendation

The Deputy Commissioner for Modernization & Chief Information Officer should:

1. Ensure that the progress in timely developing and updating mainframe access control standards, such as law enforcement manuals and access control matrices, is overseen and tracked by MITS Services management, such as through inclusion in the quarterly MITS BPRs.

Management's Response: Responsible Security Policy Support and Oversight staffs will include proposed updates of standards in their respective tactical plans for each fiscal year and update them quarterly. Further, the Security Policy Support and Oversight organization has established a policy configuration control board as part of their monitoring and change management procedures. The Office of Security Policy Support and Oversight will also complete oversight reviews to determine whether access matrices exist and comply with standard access control principles (separation of duties, least privilege access, and business need to know). Office of Security Services management will monitor these actions on a quarterly basis.

System Software Controls Could Be Monitored More Efficiently and Effectively Using Automated Tools

As stated previously, TIGTA audits have found the controls over the operating system software configuration of the IRS' OS/390-based mainframe computers to be generally adequate. However, we identified two areas where improvements in the controls over key system software

libraries (e.g., Application Program Facility libraries) for several mainframe computers are needed. These libraries contain powerful programs that could adversely affect the security and integrity of an OS/390-based mainframe computer. Specifically, we identified libraries where duplicate program names were used, which increases the possibility of programs bypassing security controls or executing an outdated copy of a program. In addition, we found that the list used to manage these libraries was incomplete, which introduces the risk that another program could be substituted and possibly circumvent security controls.

IRS management concurred with our findings and agreed to correct them as well as develop procedures to periodically review the contents of these libraries. The IRS has implemented corrective actions on two mainframe computers and is scheduled to implement corrective actions on the remaining computers by September 2002.

These weaknesses resulted from the lack of specific policies or guidance on managing the contents of these key system software libraries. However, the IRS also does not have an effective or efficient way to monitor system software controls on OS/390-based mainframe computers. The TIGTA evaluated system software controls using an automated monitoring tool that scans system software. During our audits, the IRS was not using an automated tool to monitor these computers.

The use of a system software-monitoring tool would greatly increase the IRS' ability to continue to maintain adequate system software control, through the automation of routine analysis and monitoring of the key system software components. This would enable systems programming and security personnel to more efficiently identify system software issues and focus their efforts on resolving those issues, therefore providing additional time to devote to other priorities.

GAO guidelines state that controls over access to and modification of system software are essential in providing reasonable assurance that system software controls are not compromised and that the system will not be impaired.

Inadequate controls in this area could lead to unauthorized access and circumvention of security controls to read, modify, or delete critical or sensitive information and programs and could result in the shutdown of a mainframe computer. Since the IRS' OS/390-based mainframe computers are critical to its tax and administrative processing functions, prolonged outages would result, at a minimum, in lost productivity and negative publicity for the agency.

Recommendation

The Chief, Information Technology Services should:

2. Evaluate the use of automated tools to more effectively monitor and maintain the operating system software on the IRS' mainframe computers and establish operating procedures for using such tools to periodically monitor mainframe operating system software.

Management's Response: The Director, Enterprise Operations will evaluate the use of automated tools to more effectively monitor and maintain the operating system software on the IRS' mainframe computers. In addition, the Director, Enterprise Operations will establish operating procedures for using automated tools to periodically monitor mainframe operating system software.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to analyze previously issued Treasury Inspector General for Tax Administration (TIGTA) audit reports and related corrective actions to determine whether issues presented in these reports, when viewed as a whole, indicate the need for broader corrective actions across all mainframe computer environments.

Information contained in this report was based on the following TIGTA reports issued from August 1999 to June 2002 on the adequacy of the system-level controls over the Internal Revenue Service's mainframe computers:

- *The General Controls Environment Over the Internal Revenue Service's Unisys 2200 Systems Can Be Improved* (Reference Number 1999-20-063, dated August 1999)
- *The Internal Revenue Service Can Increase Storage Capacity on Several IBM Mainframe Systems Through Improved Maintenance* (Reference Number 2000-20-009, dated November 1999)
- *The General Controls Over a Critical Internal Revenue Service Tax Processing Computer System Can Be Strengthened* (Reference Number 2000-20-072, dated May 2000)
- *The Control Environment Over the Consolidated Computer System for Collection Activities Needs to Be Strengthened* (Reference Number 2001-20-034, dated December 2000)
- *Controls Over the Masterfile System Are Generally Adequate, But Some Improvement Is Needed* (Report Number 2001-20-092, dated June 2001)
- *The System-Level Controls Over the Security and Communications System Are Adequate; However, Improvements Can Be Made* (Reference Number 2002-20-044, dated January 2002)
- *System-Level Controls Over the Detroit Computing Center Mainframe Computers Are Generally Adequate, But Some Improvement Is Needed* (Reference Number 2002-20-082, dated April 2002)
- *Management Advisory Report: The Configuration of a Security and Communications System Backup Computer Environment Is Not Compliant With Internal Revenue Service Requirements* (Reference Number 2002-20-109, dated June 2002)

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Gary Hinkle, Director
Michael Howard, Acting Audit Manager
Tina Wong, Auditor

Appendix III

Report Distribution List

Commissioner N:C
Deputy Commissioner N:DC
Chief, Information Technology Services M:I
Director, Office of Security Services M:S
Director, Enterprise Computing Centers M:I:E
Director, Enterprise Operations M:I:EO
Director, Enterprise Technical Support Services M:I:E
Director, Detroit Computing Center M:I:E:DC
Director, Martinsburg Computing Center M:I:E:MC
Director, Systems Support Division M:I:E:SS
Director, Tennessee Computing Center M:I:E:TC
Manager, Program Oversight and Coordination M:SP:P:O
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management Controls N:CFO:F:M
Audit Liaisons: Enterprise Operations M:I:EO
Office of Security Services M:S

Appendix IV

Status of Corrective Actions

The following table summarizes the June 2002 status of the Internal Revenue Service's (IRS) corrective actions to Treasury Inspector General for Tax Administration (TIGTA) final reports regarding system-level controls over the IRS' mainframe computers:

**Status of the IRS' Corrective Actions to TIGTA Final Reports
Regarding System-Level Controls Over the IRS' Mainframe Computers**

Report Number	Report Issued Date	TIGTA Recommendations	IRS' Planned Corrective Actions	Completed Corrective Actions
1999-20-063	August 1999	11	16	9
2000-20-009	November 1999	1	1	1
2000-20-072	May 2000	11	13	3
2001-20-034	December 2000	3	3	3
2001-20-092	June 2001	9	14	12
2002-20-044	January 2002	10	25	4
2002-20-082	April 2002	8	11	2
2002-20-109	June 2002	2	2	2
Totals		**55**	**85**	**36**

Source: The Department of the Treasury's Inventory, Tracking, and Closure System.

While many of the corrective actions to these reports are not yet due to be completed, due dates for other actions have been delayed. As the following table illustrates, some of these delays will result in corrective actions being completed over a year after the TIGTA's report was issued:

Summary of Delays in Corrective Action Due Dates

Status of the IRS' Corrective Actions	No change in corrective action due date	Corrective action due date delayed
Completed prior to the report issuance date	13	0
Completed in less than one year from the report issuance date	14	2
Completed in more than one year from the report issuance date	2	5
Outstanding, to be completed in less than one year from the report issuance date	23	5
Outstanding, to be completed more than one year from the report issuance date	2	19
Totals	**54**	**31**

Source: The Department of the Treasury's Inventory, Tracking, and Closure System.

Appendix V

Management's Response to the Draft Report

CHIEF
INFORMATION TECHNOLOGY SERVICES

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

AUG 27 2002

RECEIVED
AUG 28 2002

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: Terri L. Zimmerman
Chief, Information Technology Services

SUBJECT: Response to Draft Audit Report - System-Level Controls for the Internal Revenue Service's Mainframe Computers Are Generally Adequate; However, Additional Actions Are Needed (Audit # 200220003)

The Modernization, Information Technology & Security (MITS) Services organization is committed to ensuring the security and integrity of sensitive taxpayer information. One of the key means to protect this information is through system level controls of access to our mainframe computer systems. The IRS' mainframe computers are vital to accomplishing our mission. Access controls ensure employee actions are appropriate, and as such, are a critical component of IRS' customer service efforts.

The TIGTA determined we had adequate user access controls that protected most of the sensitive programs and data on the IRS' mainframe computers. The IRS has made updated access control standards for mainframe computers a priority monitored by MITS Services executive management. Updated standards protect taxpayer information and support the disaster recovery effort.

We are evaluating software monitoring tools to ensure adequate control of our key libraries of computer programs. These tools automate routine analysis and monitoring of the key system software, enabling staff to identify and resolve system software issues more efficiently. We will establish operating procedures to monitor mainframe software using these tools.

I included additional details in my attached management response. If you have any questions, please call me at (202) 622-6800, or Thomas Mulcahy, Manager, Program Oversight and Coordination Office, at (202) 283-6063.

Attachment

Attachment

Response To Draft Audit Report – System-Level Controls for the Internal Revenue Service's Mainframe Computers Are Generally Adequate; However, Additional Actions Are Needed (Audit # 200220003)

Recommendation #1
The Deputy Commissioner for Modernization & Chief Information Officer should: Ensure that the progress in timely developing and updating mainframe access control standards, such as law enforcement manuals and access control matrices, is overseen and tracked by MITS Services management, such as through inclusion in the quarterly MITS Business Performance Reviews (BPR's).

Assessment of Cause
Access controls for IRS mainframe computers are complex, and we must adequately assess and document them before implementation. They are subject to change when we add or update operating systems and applications and when customer needs change. Timely issuance of standards helps ensure that MITS Services implements and maintains adequate levels of security on its computer systems. We need to emphasize updating access standards when substantive changes occur.

Corrective Actions #1a and #1b
1a. The Director, Security Policy Support and Oversight, ensures mainframe access control standards (i.e., Internal Revenue Manual handbooks and law enforcement manuals) are developed and updated. We continually review standards to determine when substantive changes have occurred and the access control standards require updating. Responsible Security Policy Support and Oversight staffs will include proposed updates of standards in their respective tactical plans for each fiscal year and update them quarterly. Further, the Security Policy Support and Oversight organization has established a policy configuration control board as part of our monitoring and change management procedures.

1b. The Office of Security Policy Support and Oversight will complete oversight reviews to determine whether access matrices exist and comply with standard access control principles (separation of duties, least privilege access, and business need to know).

The Director, Systems Support Division, Information Technology Services, coordinates the preparation and maintenance of access matrices for IBM mainframe computer systems. Systems programming staffs for each IBM system lead a team effort that includes Computing Center security administrators, Computing Center Operational staffs and other impacted system users to determine appropriate levels of access to their respective system.

We have not baselined, the access matrices of the Unisys mainframes. The Office of Security Policy Support and Oversight is coordinating the initial development of the matrix with System Support Division, Computing Center security administrators,

Attachment

Response To Draft Audit Report – System-Level Controls for the Internal Revenue Service's Mainframe Computers Are Generally Adequate; However, Additional Actions Are Needed (Audit # 200220003)

Computing Center Operational staffs, and other impacted system users. When we basline the matrices, we will transfer maintenance to the Director, Systems Support Division or the organization designated by the Model Office taskforce.

Implementation Date of Corrective Actions #1a and #1b

Completed: **Proposed:** January 01, 2003

Responsible Official for Corrective Actions #1a and #1b
Deputy Commissioner for Modernization & Chief Information Officer M
Chief, Security Services M:S
Director, Security Policy Support and Oversight M:S:S

Monitoring Plan for Corrective Action #1a
Beginning with the tactical plans for FY 2003, the Chief, Security Services will review the updated tactical plans quarterly, providing feedback, as appropriate.

Monitoring Plan for Corrective Action #1b
The Director, Office of Security Policy Support and Oversight will review the status of access matrices quarterly, and provide feedback as needed.

Recommendation #2
The Chief, Information Technology Services should:
Evaluate the use of automated tools to more effectively monitor and maintain the operating system software on the IRS' mainframe computers and establish operating procedures for using such tools to periodically monitor mainframe operating system software.

Assessment of Cause
TIGTA identified weaknesses from the lack of specific guidance on managing the contents of key system software libraries. The use of a system software-monitoring tool would greatly increase the IRS' ability to maintain adequate system software control through automation of routine analysis and monitoring of the key system software components. This would enable systems programming and security personnel to more efficiently identify system software issues.

Corrective Actions #2a and #2b
2a. The Director, Enterprise Operations will evaluate the use of automated tools to more effectively monitor and maintain the IRS' mainframe computers operating system software.

Attachment

Response To Draft Audit Report – System-Level Controls for the Internal Revenue Service's Mainframe Computers Are Generally Adequate; However, Additional Actions Are Needed (Audit # 200220003)

2b. The Director, Enterprise Operations will establish operating procedures for using automated tools to periodically monitor mainframe operating system software.

Implementation Dates of Corrective Actions #2a and #2b

2a. Completed: **Proposed:** February 01, 2003

2b. Completed: **Proposed:** June 01, 2003

Responsible Official for Corrective Actions #2a and #2b
Deputy Commissioner for Modernization & Chief Information Officer M
Chief, Information Technology Services M:I
Director, Enterprise Operations M:I:EO

Corrective Action Monitoring Plan
Management will routinely monitor the use of automated tools by reviewing logs or other documentation, and providing appropriate feedback to improve its effectiveness.